WireGuard

Dogłębna analiza

Wojtek Mańka

- MTCNA i MTC*E
- W branży IT od 10 lat
- Administracja siecią ISP z ilością końcówek >40k
- Outsourcing klientów firmowych, korporacyjnych oraz „public” i „gov”
- Próbowałem zaprzyjaźnić się z Ubi…. serio

WireGuard… najważniejsze kwestie

- Jeden z najpopularniejszych projektów w świecie IT w ostatnich latach
- OpenSource
- Wykorzystuje protokół UDP
- Posiada dedykowaną aplikację na zdecydowaną większość platform systemowych
- Zapewnia bardzo lekką transmisję
- Jest częścią kernela („jądra systemów linuxowych”) od wersji 5.6
- Jest gotowcem co rozwiązuje problemy implementacji przez różnych vendorów
- Najbardziej „dostępny niekomercyjny VPN”

WireGuard – kwestie bezpieczeństwa

- Szyfrowanie ChaCha20 i uwierzytelnianie Poly1305
- UDP na dowolnym porcie
- Wymagamy zautentykowanej odpowiedzi od peera od pierwszej jego odpowiedzi.
- W przypadku wysłania niepoprawnego pakietu serwer w ogólnie nie odpowie.
- Używanie znaczników czasu w wszystkich wiadomościach aby wykluczyć próby podszycia się powodujące rozłączenie peera.

- Dla chętnych: https://www.wireguard.com/protocol/

WireGuard w RouterOS

- Obecny od początku RouterOS v7
- Jest częścią pakietu system
- Nie jest objęty licencjonowaniem
- Brak jawnego wsparcia sprzętowego

Co mnie boli

- Automatyczna integracja WireGuard w rozwiązaniu z Active Directory
- Musi zapalić za pierwszym… bo logi nie są szczególnie sensowne
- Wyłączenie peera nie powoduje jego odłączenia (dyskusyjne)

Czas na LAB

Dziękuję za uwagę

mikrotikon.pl

kontakt@mikrotechnology.pl